Title	$ \mathbb{Q}$の無限次代数拡大体のdefinable setについて (モデル理論と代数幾何の交流)
Author(s)	福崎, 賢治
Citation	数理解析研究所講究録 (2003), 1344: 57-63
Issue Date	2003-10
URL	http://hdl.handle.net/2433/43518
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録 1344 巻 2003 年 57-63

$\mathbb{Q}$の無限次代数拡大体のdefinable setについて

鹿児島国際大学国際文化学部　福崎賢治 (Kenji Fukuzaki)
Faculty of Intercultural Studies,
The international University of Kagoshima

1　はじめに

Julia Robinson ([1]) は1959年数体 ($\mathbb{Q}$の有限次代数拡大体) の中で$\mathbb{N}$が (よって$\mathbb{Z},\mathbb{Q}$も) $\emptyset$-definableである事を示した。従って次の疑問が自然に起こってくる。

Question 1 $\mathbb{Q}$の無限次代数拡大体で$\mathbb{N}$は *($\emptyset$-)definable* か？

勿論$\overline{\mathbb{Q}}$では当然に$\mathbb{N}$はdefinableでなく、$R=\mathbb{R}\cap\overline{\mathbb{Q}}$では$\emptyset$-definableでない。従って他の$\mathbb{Q}$の無限次代数拡大体について疑問が生じる。以下Julia Robinsonの証明を紹介し、その途中までが簡単な (多分最も簡単な) $\mathbb{Q}$の無限次代数拡大体について同様に成り立つことを示す。

2　Julia Robinsonの証明

証明は2段階に分かれている。

1. 任意の数体の代数的整数環の中で$\mathbb{N}$は$\emptyset$-definableである。
2. 任意の数体の中でその代数的整数環は$\emptyset$-definableである。

こでは2の証明を簡単に紹介する。以下Fを数体，$\mathfrak{O}$をFの代数的整数環，$\mathfrak{p}$等は$\mathfrak{O}$の素イデアルまたは付値を示す事にする。キーとなる定理は次のものである。

Theorem 2 mをすべての素イデアル$\mathfrak{p}$に対して$\mathfrak{p}^m\not| 2$となる自然数として，次の *formula* を$\varphi(a,b,c)$で表わす。

$$\exists x,y,z(1-abc^{2m}=x^2-ay^2-bz^2)$$

さらに$\psi(t)$は次の *formula* を表わす事にする。

$$\forall a,b(\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))\to\varphi(a,b,t))$$

すると$\mathbb{Z}\subseteq\psi(F)\subseteq\mathfrak{O}$である。

任意のa,bに対してFで$\varphi(a,b,0)$が成り立つから，明らかに$\psi(F)\supseteq\mathbb{N}$であり，また$F$で任意の$c$に対して$\varphi(a,b,c)\leftrightarrow\varphi(a,b,-c)$が成り立つから$\mathbb{Z}\subseteq\psi(F)$である。従って$t\in F\setminus\mathfrak{O}$を取ったとき，

$$\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))\to\varphi(a,b,t)$$

が成り立たないような$a,b\in F$を見つければよい。ここで整数論を使う。次の二つの補題がキーである。

Lemma 3 与えられた素イデアル$\mathfrak{p}_1$に対して，次を満たす$\mathfrak{O}$で互いに素な$a,b\in\mathfrak{O}$がある。

1. $(a)=\mathfrak{p}_1\cdots\mathfrak{p}_{2k}$，ここで各$\mathfrak{p}_i$は相異なり，2の素因子をすべて含む。
2. bは *totally positive prime number in* $\mathfrak{O}$で，$(a,b)_{\mathfrak{p}}=-1\iff\mathfrak{p}|a$.

Lemma 4 a,bを前の *lemma* の条件を満たすものとして，mをすべての素イデアル$\mathfrak{p}$に対して$\mathfrak{p}^m\not|2$となる自然数とすると，
$F\models\exists x,y,z(1-abc^{2m}=x^2-ay^2-bz^2)$ *iff* c *is a* $\mathfrak{p}$*-adic integer for all* $\mathfrak{p}$ *such that* $\mathfrak{p}|a$.

Proof of Theorem 2. 今$t\in F\setminus\mathfrak{O}$を取ると，ある$\mathfrak{p}_1$に対して$t$は$\mathfrak{p}_1$-adic integerではない。($\mathfrak{O}=\bigcap_{\mathfrak{p}}\mathfrak{O}_{\mathfrak{p}}$である。$\mathfrak{O}_{\mathfrak{p}}$は$F_{\mathfrak{p}}$の$\mathfrak{p}$進整数環。) この$\mathfrak{p}_1$に対してLemma 3を適用して，$a,b$を取る。Lemma 4より明らかにこの$a,b$に対して，

$$F\models\neg\varphi(a,b,t)\wedge\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))$$

であるから，Fで$\psi(t)$は成り立たない。 □

Fで$\mathfrak{O}$が$\emptyset$-definableである事は容易である。今$a_1,\ldots,a_s$を$\mathfrak{O}$のintegral basisとし（ここで$s=[F:\mathbb{Q}]$），$P_i(x)$をa_iの$\mathbb{Q}$上の最小多項式（従って$\mathbb{Z}$上の多項式）とすると，Fで

$$t\in\mathfrak{O}\iff\exists x_1,\ldots,x_s,y_1,\ldots,y_s(t=x_1y_1+\cdots+x_sy_s\wedge\bigwedge_i P_i(y_i)\wedge\bigwedge_i\psi(x_i))$$

が成り立つ。

Lemma 3,4の証明には以下の整数論からの事実が必要である。

Fact 5 $a,b\in\mathfrak{O}\setminus\{0\}$とし，$\mathfrak{p}$を素イデアル，$m$を$\mathfrak{p}^m\not|2$なる自然数とする。もし$a\not\equiv 0\pmod{\mathfrak{p}^2}$かつ$a\equiv b\pmod{\mathfrak{p}^{2m}}$ならば$a,b$は同じ$\mathfrak{p}$*-adic class*に属している(つまり$a/b\in F_{\mathfrak{p}}^2$)。

Fact 6 $a, b \in \mathfrak{O} \setminus \{0\}$ とする。もし $(a,b)_{\mathfrak{p}} = -1$ ならば $\mathfrak{p}$ は *Archimedean valuation* かまたは $2ab$ を割る素イデアルである。従って $(a,b)_{\mathfrak{p}} = -1$ となる *valuation* は有限個である。

ここで $(a,b)_{\mathfrak{p}}$ は Hilbert symbol である，つまり

$$(a,b)_{\mathfrak{p}} = \begin{cases} +1 & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } F_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

Fact 7 $a \in \mathfrak{O}$ として $a \| \mathfrak{p}$ （つまり $\mathfrak{p} | a$ で $\mathfrak{p}^2 \nmid a$） ならばある $b \in \mathfrak{O}$ があって $\mathfrak{p} \nmid b$ で $(a,b)_{\mathfrak{p}} = -1$.

Fact 8 $a, b \in F^*$ に対して，$(a,b)_{\mathfrak{p}} = -1$ となるのは偶数個の *valuation* に対してである。

Fact 9 各イデアル類（*ideal class*）には無限個の素イデアルがある。

ideal class とは F の 0 イデアルと異なる分数イデアル全体のなす群を 0 イデアルと異なる単項分数イデアルのなす部分群で割った剰余群の各類のことである。

Fact 10 $a \in \mathfrak{O}$ がイデアル $\mathfrak{m}$ と互いに素ならば，$p \equiv a \pmod{\mathfrak{m}}$ であるような総正（*totally positive*）な素元 p が無限個ある。

p が totally positive とは p の $\mathbb{Q}$ 上共役なもののうち実なものすべてが正である事である。

Fact 11 $h \in F^*$ が F で $x^2 - ay^2 - bz^2$ の形に表わされる $\Longleftrightarrow$ $(a,b)_{\mathfrak{p}} = -1$ であるような $\mathfrak{p}$ に対して h が $-ab$ と同じ $\mathfrak{p}$-*adic class* に属さない。

Proof of Lemma 3. $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k-1}$ を 2 の素因子すべてを含む相異なる素イデアルの集合とする。$\mathfrak{K}$ を積 $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k-1}$ を含む ideal class とする。Fact 9 より各 $\mathfrak{p}_i$ と異なる $\mathfrak{p}_{2k}$ を ideal class $\mathfrak{K}^{-1}$ から取る事ができる。すると $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ は単項イデアルである。a をその生成元とする。つまり，$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$.

次に b を決める。Fact 7 より，各 $i = 1, \ldots, 2k$ に対して $\mathfrak{O}$ から b_i を $\mathfrak{p}_i \nmid b_i$ で $(a,b)_{\mathfrak{p}} = -1$ であるように取れる。m をすべての素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}^m \nmid 2$ となる自然数とする。Fact 5 より，もし

$$x \equiv b_i \pmod{\mathfrak{p}_i^{2m}} \quad \text{for } i = 1, \ldots, 2k$$

ならば x と b_i は同じ $\mathfrak{p}_i$-adic class に入るので，各 i に対して $(a,x)_{\mathfrak{p}_i} = -1$ である。Chinese Remainder Theorem より，上の連立合同式は $\mathfrak{p}_1^{2m}\cdots\mathfrak{p}_{2k}^{2m}$ を法としてただ1つの解 $c \in \mathfrak{O}$ を持つ。c は $\mathfrak{p}_1^{2m}\cdots\mathfrak{p}_{2k}^{2m}$ と互いに素である。Fact 10 より，

$$p \equiv c \pmod{\mathfrak{p}_1^{2m}\cdots\mathfrak{p}_{2k}^{2m}}$$

なる totally positive prime number $p \in D$ が無限個ある。そのうちの1つを b とする。c は a と互いに素であるから，b も a と互いに素である。

あと $(a,b)_{\mathfrak{p}} = -1 \iff \mathfrak{p}|a$ である事を示す。まず作り方より，再び Fact 5 より，$i = 1,\ldots,2k$ に対して $(a,b)_{\mathfrak{p}_i} = -1$ である。b は総正だからすべての Archimedean valuation $\mathfrak{p}$ に対して $(a,b)_{\mathfrak{p}} = +1$ である。Fact 6 より $(a,b)_{\mathfrak{p}} = -1$ となりえる valuation は $\mathfrak{p} = (b)$ だけである。しかし Fact 8 よりこれはありえない。よっていえた。 □

Remark 12 上の証明から分かるように，$(a,b)_{(b)} = +1$ である。これを次節で使う。

Proof of Lemma 4. 一般に F の元 c は共通の素因子を持たないような $u, v \in D, v \neq 0$ で $c = u/v$ と表わせる。よってこのような u, v に対して，

$$F \models \exists x,y,z(v^{2m} - abu^{2m} = x^2 - ay^2 - bz^2) \text{ iff v is prime to a}$$

を示す。

$h = v^{2m} - abu^{2m}$ とおく。Fact 11 より，
$F \models \exists x,y,z(v^{2m} - abu^{2m} = x^2 - ay^2 - bz^2)$ iff $i = 1,\ldots,2k$ に対して，h は $-ab$ と同じ $\mathfrak{p}_i$-adic class に入らない，
が成り立つ。

ある i で $\mathfrak{p}_i|v$ とする。$\mathfrak{p}_i$ は u や b を割らないから，

$$h \not\equiv 0 \pmod{\mathfrak{p}_i^2},\ h \equiv -abu^{2m} \pmod{\mathfrak{p}_i^{2m}}$$

である。Fact 5 より，h は $-abu^{2m}$ と同じ $\mathfrak{p}_i$-adic class に入っている。この class は $-ab$ の class と同じである。従って h は $x^2 - ay^2 - bz^2$ の形では表わせない。

逆に v は a と互いに素であるとする。すると h は a と互いに素であり，$\mathfrak{p}_i$ が丁度きっかり一度だけ ab を割る事より，h と $-ab$ とは同じ $\mathfrak{p}_i$-adic class には入らない。従って h は $x^2 - ay^2 - bz^2$ の形で表わせる。 □

Remark 13 上の証明は，

1. $(a) = \mathfrak{p}_1\cdots\mathfrak{p}_{2k}$，ここで各 $\mathfrak{p}_i$ は相異なり，2 の素因子をすべて含む。
2. b は a と互いに素で，$(a,b)_{\mathfrak{p}} = -1 \iff \mathfrak{p}|a$.

である事だけを使っている。これを次節で使う。

3 Theorem 2の無限次代数拡大体への拡張

ζ_mを1の原始m乗根とし，lを奇素数とする。$F_0=\mathbb{Q}$，$n>0$に対して$F_n=\mathbb{Q}(\zeta_{l^n})$として，$K=\bigcup_n F_n$とおくと，$F_0\subset F_1\subset F_2\subset\cdots$であり，$K$は$\mathbb{Q}$の無限次Abel拡大である。$\mathfrak{O}_n$を$F_n$の代数的整数環とすれば$K$の代数的整数のなす環は$\mathfrak{O}_K=\bigcup_n\mathfrak{O}_n$である。本節では次の定理を証明する。

Theorem 14 次の*formula*を$\varphi(a,b,c)$で表わす。

$$\exists x,y,z(1-abc^4=x^2-ay^2-bz^2)$$

さらに$\psi(t)$は次の*formula*を表わす事にする。

$$\forall a,b(\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))\to\varphi(a,b,t))$$

すると$\mathbb{Z}\subseteq\psi(K)\subseteq\mathfrak{O}_K$である。

証明には次の円分体に関する事実を使う。

Fact 15 $0<i<j$とし，$\mathfrak{p}$をF_iの素イデアルとする。

1. $\mathfrak{p}\nmid l$ならば，$\mathfrak{p}$のF_jでの素因子分解は，$\mathfrak{p}=\mathfrak{P}_1\cdots\mathfrak{P}_g$. ここで$g$は$[F_j:F_i]=l^{j-i}$の約数である。

2. $\mathfrak{p}|l$ならば，$\mathfrak{p}$のF_jでの素因子分解は，$\mathfrak{p}=\mathfrak{P}^{j-i}$. ここで$\mathfrak{p}=(1-\zeta_{l^i}),\mathfrak{P}=(1-\zeta_{l^j})$である。

Fact 16 $0<i<j$とし，$a,b\in F_i$，$\mathfrak{p}$をF_iの素イデアルとし，$\mathfrak{P}$をF_jでの$\mathfrak{p}$の素因子とする。
$(a,b)_{\mathfrak{p}}=-1$ならば$(a,b)_{\mathfrak{P}}=-1$であり，$(a,b)_{\mathfrak{p}}=+1$ならば$(a,b)_{\mathfrak{P}}=+1$である。

一般に，次の事が成り立つ。

1. $(a_1a_2,b)_{\mathfrak{p}}=(a_1,b)_{\mathfrak{p}}(a_2,b)_{\mathfrak{p}}$

2. K,kを数体とし，$K_{\mathfrak{P}}/k_{\mathfrak{p}}$が有限次拡大，$b\in k_{\mathfrak{p}},\alpha\in K_{\mathfrak{P}},a=N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\alpha)$とすると，$(\alpha,b)_{\mathfrak{P}}=(a,b)_{\mathfrak{p}}$.

ここで$0<i<j$とすると，$(F_j)_{\mathfrak{p}}/(F_i)_{\mathfrak{P}}$は次数が$[F_j:F_i]=l^{j-i}$を割り切る有限次拡大である。次数を$u$とすると$N_{(F_j)_{\mathfrak{P}}/(F_i)_{\mathfrak{p}}}(a)=a^u$だから，上の事実より$(a,b)_{\mathfrak{P}}=(a,b)_{\mathfrak{p}}^u$となる。$u$は奇数よりFact 16が出る。

Proof of Theorem 14. $\mathbb{Z}\subseteq\psi(K)$は明らかである。今$t\in K\setminus\mathfrak{O}_K$を取る。$t$を含む$F_n$を1つ固定する。$n>1$に取る。

するとあるF_nの素イデアル$\mathfrak{p}_1$に対して，tは$\mathfrak{p}_1$-adic integerではない。この$\mathfrak{p}_1$に対してLemma 3を適用して，$\mathfrak{O}_n$からa,bを取る。

1. $(a)=\mathfrak{p}_1\cdots\mathfrak{p}_{2k}$，ここで各$\mathfrak{p}_i$は相異なり，2の素因子をすべて含む。

2. bはtotally positive prime number in $\mathfrak{O}$で，$(a,b)_{\mathfrak{p}}=-1\iff\mathfrak{p}|a$.

であるが，$\mathfrak{p}_2,\ldots,\mathfrak{p}_{2k}$の各素因子は素数$l$を割らないように取れる。

F_nではFact 15より，すべての素イデアル$\mathfrak{p}$に対して$\mathfrak{p}^2\nmid 2$だから前節のLemma 4より$1-abt^4=x^2-ay^2-bz^2$は解x,y,zをF_nに持たない。

あと$s>n$として，この等式がF_sでも解x,y,zを持たない事をいえばよい。$s-n$を偶数に取る。

case 1. $\mathfrak{p}_1$が素数lの素因子でないとき:

まず$a,b\in\mathfrak{O}_s$でaとbは$\mathfrak{O}_n$で互いに素であるから，$\mathfrak{O}_s$でも互いに素である。

Fact 15よりF_sでの素因子分解は，

1. $(a)=\mathfrak{P}_1\cdots\mathfrak{P}_{2r}$，ここで各$\mathfrak{P}_i$は相異なり，2の素因子をすべて含む。

となる。

またbはF_sでも総正であることと，Remark 12とFact 16より

2. aとbは$\mathfrak{O}_n$で互いに素で，$(a,b)_{\mathfrak{P}}=-1\iff\mathfrak{P}|a$.

がいえる。Remark 13より，mを2としたLemma 4がF_sで成り立ち，同じようにして，$1-abt^4=x^2-ay^2-bz^2$は解x,y,zをF_sに持たない。

case 2. $\mathfrak{p}_1$が素数lの素因子であるとき:

Fact 15よりF_sでのaの素因子分解は，

1. $(a)=\mathfrak{P}_1^{l^{s-n}}\cdots\mathfrak{P}_{2r'}$，ここで各$\mathfrak{P}_i$は相異なり，2の素因子をすべて含む。

となる。Fact 15より$\mathfrak{P}_1=(1-\zeta_{l^s})$である。$a'=a/(1-\zeta_{l^s})^{l^{s-n}-1}$とおくと，

1. $(a')=\mathfrak{P}_1\cdots\mathfrak{P}_{2r'}$，ここで各$\mathfrak{P}_i$は相異なり，2の素因子をすべて含む。

次に$a=a'((1-\zeta_{l^s})^{(l^{s-n}-1)/2})^2$より，各$i$に対して$(a,b)_{\mathfrak{P}}=(a',b)_{\mathfrak{P}}$である。

（$(l^{s-n}-1)/2$は整数）よって，

2. a' と b は $\mathfrak{O}_s$ で互いに素で，$(a',b)_{\mathfrak{P}}=-1 \Longleftrightarrow \mathfrak{P}|a'$.

従って同様に，

$1-a'bc^4=x^2-a'y^2-bz^2$ は解 x,y,z を F_s に持つ $\Longleftrightarrow$ c は $\mathfrak{P}|a'$ なる $\mathfrak{P}$ に対して $\mathfrak{P}$-adic integer, が成り立つ。

今 $1-abt^4=x^2-ay^2-bz^2$ が解 x,y,z を F_s に持つとする。$s-n$ が偶数より $(l^{s-n}-1)/4$ は整数だから，

$$1-a'b(t(1-\zeta_{l^s})^{(l^{s-n}-1)/4})^4=x^2-a'((1-\zeta_{l^s})^{(l^{s-n}-1)/2}y)^2-bz^2$$

が解 x,y,z を F_s に持つことになる。しかし $t(1-\zeta_{l^s})^{(l^{s-n}-1)/4}$ は $\mathfrak{P}_1$ に対して $\mathfrak{P}_1$-adic integer にならないから矛盾する。よってこのときも $1-abt^4=x^2-ay^2-bz^2$ は解 x,y,z を F_s に持たない。 □

4 終わりに

J.Robinson([1]) の方法では Theorem 14 がいえてもそこから $\mathfrak{O}_K$ の definability は出てこない。しかし無限次代数拡大体 K は算術性を色濃く持った体といえる。ちなみに $\overline{\mathbb{Q}}$ はまったく算術性のない体といえる。従って K はその中で $\mathbb{N}$ を定義できる可能性があるものと思われる。

参考文献

[1] Robinson, J., *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc., 10, pp 950-957, 1959.